PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

(Chapter II of the Patent Cooperation Treaty)

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference PU030228	**FOR FURTHER ACTION**	See Form PCT/IPEA/416
International application No. PCT/US2004/024559	International filing date *(day/month/year)* 29.07.2004	Priority date *(day/month/year)* 29.07.2003

International Patent Classification (IPC) or national classification and IPC

H04L29/06

Applicant

THOMSON LICENSING S.A. et al.

1. This report is the international preliminary examination report, established by this International Preliminary Examining Authority under Article 35 and transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 6 sheets, including this cover sheet.

3. This report is also accompanied by ANNEXES, comprising:

    a. ☒ *sent to the applicant and to the International Bureau)* a total of 6 sheets, as follows:

    ☒ sheets of the description, claims and/or drawings which have been amended and are the basis of this report and/or sheets containing rectifications authorized by this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions).

    ☐ sheets which supersede earlier sheets, but which this Authority considers contain an amendment that goes beyond the disclosure in the international application as filed, as indicated in item 4 of Box No. I and the Supplemental Box.

    b. ☐ *(sent to the International Bureau only)* a total of (indicate type and number of electronic carrier(s)) , containing a sequence listing and/or tables related thereto, in computer readable form only, as indicated in the Supplemental Box Relating to Sequence Listing (see Section 802 of the Administrative Instructions).

4. This report contains indications relating to the following items:

    ☒ Box No. I Basis of the opinion

    ☒ Box No. II Priority

    ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

    ☐ Box No. IV Lack of unity of invention

    ☒ Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

    ☐ Box No. VI Certain documents cited

    ☐ Box No. VII Certain defects in the international application

    ☐ Box No. VIII Certain observations on the international application

Date of submission of the demand 12.04.2005	Date of completion of this report 26.10.2005
Name and mailing address of the international preliminary examining authority: European Patent Office - Gitschiner Str. 103 D-10958 Berlin Tel. +49 30 25901 - 0 Fax: +49 30 25901 - 840	Authorized Officer Figiel, B Telephone No. +49 30 25901-473

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No.
PCT/US2004/024559

IAP20 Rec'd PCT/PTO 27 JAN 2006

Box No. I Basis of the report

1. With regard to the **language**, this report is based on the international application in the language in which it was filed, unless otherwise indicated under this item.

   ☐ This report is based on translations from the original language into the following language , which is the language of a translation furnished for the purposes of:
   ☐ international search (under Rules 12.3 and 23.1(b))
   ☐ publication of the international application (under Rule 12.4)
   ☐ international preliminary examination (under Rules 55.2 and/or 55.3)

2. With regard to the **elements*** of the international application, this report is based on *(replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report)*:

   Description, Pages

   1-10   as originally filed

   Claims, Numbers

   1-41   received on 12.04.2005 with letter of 12.04.2005

   Drawings, Sheets

   1-3   as originally filed

   ☐ a sequence listing and/or any related table(s) - see Supplemental Box Relating to Sequence Listing

3. ☐ The amendments have resulted in the cancellation of:
   ☐ the description, pages
   ☐ the claims, Nos.
   ☐ the drawings, sheets/figs
   ☐ the sequence listing *(specify)*:
   ☐ any table(s) related to sequence listing *(specify)*:

4. ☒ This report has been established as if (some of) the amendments annexed to this report and listed below had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).
   ☐ the description, pages
   ☒ the claims, Nos. 14-24,35,37-40
   ☐ the drawings, sheets/figs
   ☐ the sequence listing *(specify)*:
   ☐ any table(s) related to sequence listing *(specify)*:

   *   If item 4 applies, some or all of these sheets may be marked "superseded."

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

Box No. II   Priority

1. ☒ This report has been established as if no priority had been claimed due to the failure to furnish within the prescribed time limit the requested:

   ☒ copy of the earlier application whose priority has been claimed (Rule 66.7(a)).

   ☐ translation of the earlier application whose priority has been claimed (Rule 66.7(b)).

2. ☐ This report has been established as if no priority had been claimed due to the fact that the priority claim has been found invalid (Rule 64.1). Thus for the purposes of this report, the international filing date indicated above is considered to be the relevant date.

3. Additional observations, if necessary:

Box No. V   Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-13,25-34,36,41
	No:	Claims	
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-13,25-34,36,41
Industrial applicability (IA)	Yes:	Claims	1-13,25-34,36,41
	No:	Claims	

2. Citations and explanations (Rule 70.7):

   see separate sheet

**INTERNATIONAL PRELIMINARY
REPORT ON PATENTABILITY
(SEPARATE SHEET)**

10/566393

IAP20 Rec'd PCT/PTO 27 JAN 2006

International application No.

PCT/US2004/024559

V. Reasoned statement under Art. 35(2)

1. Reference is made to the following documents; the numbering will be adhered to in the rest of the procedure:

    D1: WO 96/42041 A (OPEN MARKET INC) 27 December 1996 (1996-12-27)

2. The application does not meet the requirements of **Article 6 PCT**, because the independent **claims 1 and 25** are not clear:

2.1 In claim 1 it is not clear which entities perform the steps of *"transmitting an authentication request"* and *"receiving a response to said authentication request"*. It is assumed that they are performed by the client (as in the figure 3).

2.2 Similar objection is to be raised for claim 25 for the corresponding features.

3. The present application does not meet the criteria of **Article 33(1) PCT**, because the subject-matter of **independent claims 1 and 25** does not involve an inventive step in the sense of Article 33(3) PCT.

3.1 Referring to the wording of **claim 1** document D1 discloses:
    a method for controlling access to a network (abstract); said method comprising:
    -   receiving, by an access point of said network, a request to access said network, said request transmitted by a client (Get CP: figure 3, step 3);
    -   re-directing, by said AP, said access request to a local server (this step can be omitted in the case that AP and local server are co-located - one of two straightforward possibilities);
    -   generating an URL by said AP/local server requesting that said client select an authentication server (AS) and forwarding said generated URL to said client (Redirect [AS]: figure 3, step 4; page 14, lines 6-8; it is **to be noted** that for the purpose of the authentication it is not relevant if such URL to the authentication server is sent directly to the user or if it is embedded in Web page and than sent to the user);
    -   transmitting an authentication request to said selected authentication server

([AS] Get CP: figure 3, step 5; page 14, lines 8-13);

- receiving a response to said authentication request from said selected authentication server (New URL w/SID: figure 3, step 8; page 14, line 34 - page 15, line 1).

- storing a mapping of an association of unique data with an identifier of said client in said AP (page 15, lines 3-5);

3.2   From the method disclosed in document D1 the subject matter of **claim 1** differs in that AP/local server associates/generates the unique data with an identifier of said client. The problem to be solve is to generate a challenge which can be authenticated by other trusted party.
This feature is merely one of the straightforward possibilities from which the skilled person would select in accordance with circumstances, without the exercise of inventive skill, in order to solve the problem posed. Applying of session ID and randomized number for the authentication is very well known in the art and used e.g. in the IEEE 802.1x systems (see description, page 14, lines 13-14).

3.3   Furthermore it is **to be noted** that the problem to be solved by the present application is **to authenticate a user** without requiring an explicit separate communication session between the access point and the authentication server (see description page 3, lines 3-6 and 29-32). Document D1 provides exact the same solution. The mere fact that an access to the service instead of an access to the network is controlled it is regarded as irrelevant.

Thus, the subject-matter of claim 1 does not involve an inventive step and does not satisfy the criterion set forth in Articles 33(1) and 33(3) PCT.

3.4   The above-mentioned lack of clarity notwithstanding, referring to the wording of **claim 25,** as far as it can be construed, document D1 discloses:
a system for controlling access to a network comprising:
i)   a client (client 50, figure 3);
ii)   an access point AP co-located with a local server LS for relaying network communications to and from the client (content server 52, figure 3); and
iii)   an authentication server (54, figure 3) for performing an authentication process

in response to a request from the client; wherein
- the LS transmits the unique data to the client (Redirect [AS]: figure 3, step 4; page 14, lines 6-8);
- the authentication server, upon authenticating the client using the unique data (page 14, lines 14-29), is operative to provide a re-direct header for access to the client (New URL w/SID: figure 3, step 8; page 14 line 34 - page 15, line 1) including a digitally signed authentication message and authentication parameters corresponding to the unique data (page 14, lines 30-33),
- the AP receiving the digitally signed retrieved re-directed URL and authentication parameters from the client (figure 3, step 9) and the AP further correlating the authentication parameters with the mapped association data for determining access to the network based on the results of the correlation (page 14, lines 3-8).

From the method disclosed in document D1 the subject matter of claim 25 differs in that AP/local server associates/generates the unique data with an identifier of said client. This feature cannot be regarded as involving inventive step as already stated in points 3.2 and 3.3

Thus, the subject-matter of claim 25 does not involve an inventive step and does not satisfy the criterion set forth in Articles 33(1) and 33(3) PCT.

4.   The **dependent claims 2-13, 26-34, 36 and 41** do not appear to contain any additional features which, in combination with the features of any claim to which they refer, involve an inventive step (Articles 33(1) and 33(3) PCT) for the reason that the subject-matter of said claims is either in principle directly derivable from the disclosure of the document D1 or represents simple design details which are generally known to the person skilled in the field of access control.

4.1   Claims 2 and 26: the additional feature of these claims (said network is a WLAN) cannot be regarded as involving inventive step as already stated in point 3.3.

12-04-2005   15:01 FR THOMSON MM LICENSIN609 734 6888   8. 01149302590184 P 18
609 734 6888
US0424559

PU030028

10/566393

IAP20 Rec'd PCT/PTO 27 JAN 2006

11

CLAIMS:

1. A method for controlling access to a network, said method comprising:

receiving, by an access point (AP) of said network, a request to access said network, said request transmitted by a client;

re-directing, by said AP, said access request to a local server;

associating unique data with an identifier of said client and storing a mapping of said association in said AP;

generating a Web page by said local server requesting that said client select an authentication server (AS) and including said unique data and forwarding said generated Web page to said client;

transmitting an authentication request to said selected authentication server; and

receiving a response to said authentication request from said selected authentication server.

2. The method according to claim 1, wherein said network is a wireless Local Area network (WLAN).

3. The method according to claim 1, further comprising:

forwarding said identifier of said client from said local server; and

generating said unique data for said client by said local server.

4. The method according to claim 1, further comprising:

retrieving, by said client, a re-directed URL having embedded data including a first digital signature, authentication parameters and said unique data and forwarding said re-directed URL to said AP;

creating, by said AP, a second digital signature using said authentication parameters, said unique data and said identifier;

comparing, by said AP, said first digital signature with said second digital signature;

determining, by said AP, if there is a match between said first digital signature and said second digital signature; and

SUBSTITUTE SHEET

AMENDED SHEET

12

performing, by said AP, one of granting network access and denying network access based on said match determination.

5. The method according to claim 1, wherein said unique data includes a session ID and a randomized number.

6. The method according to claim 1, wherein said identifier is an address of said client.

7. The method according to claim 1, wherein the act of authenticating further comprises:

processing, by said AS, said authentication request, wherein said authentication request includes a session ID embedded in said authentication request;

responding to said authentication request by forwarding to said client by said AS an authentication input page, said authentication input page including a request for authentication information; and

receiving, by said AS, authentication credentials from said client, wherein said response to said authentication request forwarded to said client includes a re-direct header and a success code and associated information relevant to access of said network by said client.

8. The method according to claim 7, wherein the act of forwarding further comprises generating, by said AS, said success code and said associated information includes a first digital signature and authentication parameters.

9. The method according to claim 5, wherein said randomized number is one of a random number and a pseudo-random number.

10. The method according to claim 1, wherein said identifier is one of a physical (PHY) address of said client, a MAC address of said client and an IP address of said client.

11. The method according to claim 1, wherein said AP and said local server are co-located.

SUBSTITUTE SHEET

AMENDED SHEET

13

12. The method according to claim 4, wherein said first and said second digital signatures are generated using one of a private key of said AS and a shared key between said AS and said local server.

13. The method according to claim 4, wherein said second digital signature is locally generated at said AP.

Claim 14.   (CANCELLED)

Claim 15.   (CANCELLED)

Claim 16.   (CANCELLED)

Claim 17.   (CANCELLED)

Claim 18.   (CANCELLED)

Claim 19.   (CANCELLED)

Claim 20.   (CANCELLED)

Claim 21.   (CANCELLED)

Claim 22.   (CANCELLED)

Claim 23.   (CANCELLED)

Claim 24.   (CANCELLED)

25. A system for controlling access to a network comprising:
a client;

SUBSTITUTE SHEET

AMENDED SHEET

14

an access point (AP) coupled to a local server (LS) for relaying network communications to and from the client; and

an authentication server for performing an authentication process in response to a request from the client; wherein

the AP, in response to a re-directed request to access the network from the client, associates unique data with an identifier of the client and stores a mapping of the association;

the LS transmits the unique data to the client;

the authentication server, upon authenticating the client using the unique data, is operative to provide a re-direct header for access to the client including a digitally signed authentication message and authentication parameters corresponding to the unique data, the AP receiving the digitally signed retrieved re-directed URL and authentication parameters from the client and the AP further correlating the authentication parameters with the mapped association data for determining access to the network based on the results of the correlation.

26. The system of claim 25, wherein the network is a wireless local area network (WLAN) comprising the access point and local server.

27. The system of claim 25, wherein the local server generates a web page requesting that the client select an authentication server, and embeds the unique data in the web page for transmission to the client.

28. The system of claim 25, wherein the identifier of the client is one of a physical address, MAC address and an IP address, and wherein the unique data comprises a session ID and a randomized number.

29. The system of claim 28, wherein the session ID and randomized number are generated by the local server.

30. The system of claim 28, wherein the authentication server receives user credential information from the client and provides a digitally signed authentication message including

SUBSTITUTE SHEET

AMENDED SHEET

15

an authentication parameters using said unique data through HTTPS to the client via said re-direct header to the client.

31. The system of claim 30, wherein the AP, in response to receiving the digitally signed authentication message re-directed from the client including the authentication parameters and at least a portion of the unique data from the client, generates a local digital signature using the received portion of the unique data and the stored mapping data together with the authentication parameters, and compares the local digital signature with the digitally signed authentication message to determine network access by the client.

32. The system of claim 25, wherein the re-direct header further comprises a means for re-directing a browser of the client to a URL on the network, and embedding in the URL said digitally signed authentication message, the authentication parameters and a portion of the unique data.

33. The system of claim 26, wherein said AP and said LS are co-located.

34. The method of Claim 1, further comprising:
at the authentication server, authenticating the client using the unique data, and forwarding said response to the client using a re-direct header, and including a digitally signed authentication message and authentication parameters corresponding to the unique data; and
the access point receiving from the client according to the re-direct header the digitally signed authentication message and authentication parameters and correlating the authentication parameters with the mapped association data for determining access to the network.

Claim 35. (CANCELLED)

36. The method of Claim 1, wherein said unique data comprises a session ID and a randomized number and further comprising: receiving, by said AP, a re-directed request from the client and including a digitally signed authentication message, an authentication parameter list, and said session ID, the digitally signed authentication message being generated using the

SUBSTITUTE SHEET

AMENDED SHEET

16

randomized number, said session ID and said authentication parameter list, by said selected
authentication server associated with the client; and

correlating the received digitally signed authentication message with the re-
directed request for access using the stored mapping data for controlling access by the client
to the network.

Claim 37. (CANCELLED)

Claim 38. (CANCELLED)

Claim 39. (CANCELLED)

Claim 40. (CANCELLED)

41. The method according to claim 36, wherein said AP and said LS are co-located.

SUBSTITUTE SHEET

AMENDED SHEET